

Hinweise:

Handelt es sich bei den von Ihnen im Rahmen des Dienstes „CompuDMS Cloud“ gespeicherten Daten um personenbezogene Daten, so verarbeitet die CompuKöln diese Daten als Auftragsverarbeiter im Sinne des Art. 28 DSGVO ausschließlich im Auftrag und nach den Weisungen von Ihnen und ausschließlich zum Zwecke der Bereitstellung des Dienstes.

Aufgrund der gesetzlichen Vorgaben in Art. 28 DSGVO obliegt es Ihnen, mit der CompuKöln eine Vereinbarung über die Auftragsverarbeitung abzuschließen. Diese Vereinbarung haben wir nachfolgend bereits ausformuliert. Bitte haben Sie Verständnis dafür, dass wir nur auf Basis dieses vorformulierten Textes eine Vereinbarung über Auftragsverarbeitung im Rahmen von CompuDMS Cloud mit Ihnen abschließen. Sollten Sie mit dem Vereinbarungstext nicht einverstanden sein, so räumen wir Ihnen ein außerordentliches Kündigungsrecht ein.

Ergänzen Sie bitte den Vereinbarungstext auf dieser Seite um die notwendigen Angaben zu Ihrem Unternehmen und unterschreiben Sie rechtsverbindlich die Vereinbarung auf der letzten Seite unter Angabe von Ort und Datum.

*Senden Sie dann zwei unterschriebene Ausfertigungen der Vereinbarung an die **CompuKöln Dokument Management GmbH, Stollwerckstr. 5, 51149 Köln.***

Wir werden Ihnen dann eine von uns gegengezeichnete Ausfertigung zusenden.

Sollten Sie uns nur eine Ausfertigung zusenden, so werden wir sie kopieren und Ihnen die Kopie gegengezeichnet zusenden. So liegt jeder Partei die Original-Unterschrift der anderen Partei vor.

Auftragsverarbeitungsvereinbarung gemäß Art. 28 DSGVO

in Ergänzung zu den Lizenz- und Nutzungsbedingungen für die Software CompuDMS Cloud

zwischen der

CompuKöln Dokument Management GmbH
Stollwerckstraße 5, 51149 Köln

- Auftragsverarbeiter, nachfolgend „CompuKöln“ genannt –

und

[Firma]

[Straße, PLZ Ort]

- Verantwortlicher, nachfolgend „Kunde“ genannt -

1. Präambel

Diese Vereinbarung konkretisiert die Verpflichtungen der Parteien zum Datenschutz, die sich aus der in den Lizenz- und Nutzungsbedingungen für die Software CompuDMS Cloud (nachfolgend „Nutzungsbedingungen“ genannt) in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben.

2. Gegenstand und Dauer der Auftragsverarbeitung

- (1) Die CompuKöln oder durch die CompuKöln Beauftragte verarbeiten personenbezogene Daten (nachfolgend auch als „Daten“ bezeichnet) im Auftrag des Kunden (Verantwortlicher) im Sinne des Artikel 4 Abs. 2 und Artikel 28 DSGVO. Dies umfasst diejenigen Tätigkeiten, die in den Nutzungsbedingungen konkretisiert sind.
- (2) Gegenstand der Auftragsverarbeitung ist die Bereitstellung der Software zur Nutzung durch den Kunden im Wege des Zugriffs über das Internet.
- (3) Art der Daten sowie der Kategorien der Betroffenen sind durch den Kunden frei wählbar; sie umfassen (bitte ankreuzen und ggf. ergänzen):

Art der Daten:

- Name, Vorname, Geburtsname
- Familienstand
- Geburtsdatum
- Adressen
- Kontaktdaten wie Telefonnummern, E-Mailadressen
- Kontoverbindungen
- Kfz-Kennzeichen
- Personalausweisnummer
- Zeugnisse
- Personalstammdaten
- Vertragsstammdaten
- Sonstige:

Kategorien der Betroffenen:

- Kunden
 - Interessenten
 - Mitarbeiter
 - Lieferanten
 - Handelsvertreter
 - Ansprechpartner
 - sonstige soziale Kontakte
 - Mitarbeiter von Behörden
 - Sonstige:
-
-

- (4) Ausgenommen ist die Verarbeitung besonderer Kategorien personenbezogener Daten gem. Artikel 9 DSGVO. Der Kunde darf besondere Kategorien personenbezogener Daten nicht speichern. Besondere Kategorien personenbezogener Daten umfassen Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.
- (5) Die Laufzeit dieser Vereinbarung entspricht der Laufzeit des Vertrages über die Nutzung des Dienstes. Endet der Vertrag, so endet auch diese Vereinbarung.
- (6) Der Kunde ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz, insbesondere für die Rechtmäßigkeit der Datenweitergabe an die CompuKöln sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DSGVO).
- (7) Die Erbringung der vereinbarten Datenverarbeitung erfolgt ausschließlich auf Servern in der Europäischen Union. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Kunden und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.
- (8) Der Kunde hat die CompuKöln unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

3. Weisungsbefugnis des Kunden

- (1) Die CompuKöln darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Kunden verarbeiten außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DSGVO vor.
- (2) Die Datenverarbeitung durch die CompuKöln erfolgt im Rahmen der zur Verfügungstellung einer standardisierten, konfigurierbaren Software über das Internet. Der Kunde übt sein Weisungsrecht in Bezug auf die Daten entsprechend durch Einrichtung und Benutzung der Software aus. Dem Kunden bleiben darüberhinausgehende Weisungen bei gesondert zu vereinbarenden und zu vergütenden Anpassungen der Software oder Datenmigration vorbehalten.
- (3) Geht der Inhalt von Weisungen des Kunden über dasjenige hinaus, was die CompuKöln dem Kunden gemäß Nutzungsbedingungen schuldet, hat der Kunde die der Weisung folgenden Leistungen gesondert zu vergüten.
- (4) Weisungen des Kunden erfolgen grundsätzlich in schriftlicher Form oder in einem elektronischen Format (Textform). Soweit in Ausnahmefällen mündliche Weisungen erteilt werden, werden diese unverzüglich der CompuKöln in schriftlicher Form nachgereicht.
- (5) Die CompuKöln hat den Kunden unverzüglich zu informieren, wenn sie der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Die CompuKöln ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Kunden bestätigt oder geändert wird.

4. Technisch-organisatorische Maßnahmen

- (1) Die CompuKöln wird Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme umsetzen. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen. Einzelheiten dieser technisch-organisatorische Maßnahmen sind in Anlage 1 beschrieben.
- (2) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es der CompuKöln gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.
- (3) Dem Kunden sind die eingesetzten technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

5. Pflichten der CompuKöln

- (1) Die CompuKöln gewährleistet, dass es den mit der Verarbeitung der Daten des Kunden befassten Mitarbeitern und anderen für die CompuKöln tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet die CompuKöln, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.
- (2) Die CompuKöln unterrichtet den Kunden unverzüglich, wenn ihr Verletzungen des Schutzes personenbezogener Daten des Kunden bekannt werden.
- (3) Die CompuKöln berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Kunde dies anweist, dies vom Weisungsrahmen umfasst ist und die technische Möglichkeit hierfür besteht. Die CompuKöln kann dem Kunden ihre Leistungen gegen entsprechenden Leistungsnachweis sowie weitere ihr in diesem Zusammenhang entstehende Kosten berechnen.
- (4) Daten sind nach Auftragsende auf Verlangen des Kunden zu löschen.
- (5) Im Falle einer Inanspruchnahme des Kunden durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich die CompuKöln den Kunden bei der Abwehr des Anspruches im Rahmen ihrer Möglichkeiten zu unterstützen. Die CompuKöln kann dem Kunden ihre Unterstützungsleistungen gegen entsprechenden Leistungsnachweis berechnen. Sie wird den Kunden auf die Entgeltspflichtigkeit zuvor hinweisen.
- (6) Die CompuKöln darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Kunden berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an die CompuKöln wendet, wird die CompuKöln dieses Ersuchen unverzüglich an den Kunden weiterleiten.
- (7) Sollten die Daten des Kunden bei der CompuKöln durch Pfändung oder Beschlagnahme, durch ein Insolvenzverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat die CompuKöln den Kunden unverzüglich darüber zu informieren. Die CompuKöln wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Kunden als Verantwortlichem im Sinne der Datenschutz-Grundverordnung liegen.

6. Anfragen betroffener Personen

- (1) Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an die CompuKöln, wird die CompuKöln die betroffene Person an den Kunden verweisen, sofern eine Zuordnung an den Kunden nach Angaben der betroffenen Person

möglich ist. Die CompuKöln leitet den Antrag der betroffenen Person unverzüglich an den Kunden weiter. Die CompuKöln haftet nicht, wenn das Ersuchen der betroffenen Person vom Kunden nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

- (2) Die CompuKöln unterstützt soweit vereinbart den Kunden im Rahmen ihrer Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten. Die CompuKöln kann dem Kunden ihre Unterstützungsleistungen gegen entsprechenden Leistungsnachweis berechnen. Sie wird den Kunden auf die Entgeltspflichtigkeit zuvor hinweisen.

7. Nachweise und Kontrollrechte

- (1) Zum Zwecke der Kontrolle wird die CompuKöln dem Kunden auf dessen in Textform geäußerten Wunsch hin ein Selbsttestat ihres betrieblichen Datenschutzbeauftragten darüber ausstellen, dass und in welcher Form sie die vereinbarten technischen und organisatorischen Maßnahmen nach Ziffer 4 einhält.
- (2) Weitergehende Kontrollrechte hat der Kunde nur in dem Fall, dass nachweisbar Umstände eintreten, die die Annahme der mangelnden Einhaltung der Datensicherheit rechtfertigen. Stellt sich im Nachhinein heraus, dass keine mangelnde Einhaltung der Datensicherheit vorgelegen hat, so hat der Kunde die Kosten der Kontrolle einschließlich der Personalaufwände der CompuKöln zu tragen.

8. Subunternehmer (weitere Auftragsverarbeiter)

- (1) Die Beauftragung von Subunternehmern ist der CompuKöln grundsätzlich gestattet, sofern diese Subunternehmer in der Europäischen Union tätig werden.
- (2) Die CompuKöln stellt sicher, dass die Kontrollrechte des Kunden gem. Ziffer 7 durch die Einschaltung von Subunternehmern nicht eingeschränkt werden.
- (3) Die CompuKöln wird die Beauftragung eines Subunternehmers dem Kunden eine angemessene Zeit vorab schriftlich oder in Textform anzeigen. Die Weitergabe von personenbezogenen Daten des Kunden an den Subunternehmer ist zulässig, wenn der Kunde nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber der CompuKöln schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2 bis 4 DSGVO zugrunde gelegt wird.
- (4) Widerspricht der Kunde der Beauftragung eines Subunternehmers, so steht der CompuKöln ein außerordentliches Kündigungsrecht gegenüber dem Kunden zu. Auf die Regelungen der Nutzungsbedingungen zur Vertragsbeendigung wird hingewiesen.

- (5) Die Weitergabe von personenbezogenen Daten des Kunden an den Subunternehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
- (6) Mit dem Abschließen dieser Vereinbarung stimmt der Kunde der Beauftragung folgender, derzeit in Anspruch genommener Subunternehmer zu:
 - a. Amazon Web Services EMEA SARL, 38 avenue John F. Kennedy, L-1855, Luxemburg
 - b. Amazon Web Services Inc., 410 Terry Avenue North, Seattle, Washington 98109-5210, USA
 - c. Telekom Deutschland GmbH, Landgrabenweg 151, 53227 Bonn, Deutschland

Die von diesen Subunternehmern im Rahmen dieses Vertrages genutzten Rechenzentrumsdienstleistungen werden in der Europäischen Union erbracht.

9. Sonstiges

- (1) Die Haftung der Parteien richtet sich nach den gesetzlichen Vorschriften des Art. 82 DSGVO.
- (2) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen der CompuKöln – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
- (3) Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zur Auftragsverarbeitung den Regelungen der Nutzungsbedingungen vor.
- (4) Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts und der Regelungen des IPR. Als Gerichtsstand wird Köln vereinbart.
- (5) Diese Vereinbarung ersetzt gegebenenfalls nach dem BDSG in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 10 Absatz 2 des Gesetzes vom 31. Oktober 2017 (BGBl. I S. 3618) geändert worden ist, abgeschlossene Verträge über Auftragsdatenverarbeitung, insbesondere „Vereinbarungen über Auftragsdatenverarbeitung gemäß § 11 BDSG in Ergänzung zu den Lizenz- und Nutzungsbedingungen für die Software CompuDMS Cloud“.

(6) Diese Vereinbarung tritt mit ihrer Unterzeichnung in Kraft, jedoch keinesfalls vor dem 25.05.2018.

_____ Ort, Datum	_____ Köln, den
_____ Firma Kunde	_____ CompuKöln Dokument Management GmbH
_____ Unterschrift des Kunden	_____ Unterschrift
_____ Name des Unterzeichners in Druckbuchstaben	_____ Name des Unterzeichners in Druckbuchstaben

Anlage 1 - Technisch-organisatorische Maßnahmen

Die CompuKöln verpflichtet sich gegenüber dem Kunden zur Einhaltung nachfolgender technischer und organisatorischer Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind:

a) Zutrittskontrolle (Vertraulichkeit – Art. 32 Abs. 1 lit. b DSGVO)

Maßnahmen, mit denen Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird:

- Festlegung von Sicherheitsbereichen
- Verwaltung und Dokumentation von personengebundenen Zutrittsberechtigungen über den gesamten Lebenszyklus
- Begleitung von Besuchern und Fremdpersonal
- Überwachung der Räume außerhalb der Betriebszeiten
- Protokollierung des Zutritts zu den datenverarbeitenden IT-Systemen

b) Zugangskontrolle (Vertraulichkeit – Art. 32 Abs. 1 lit. b DSGVO)

Maßnahmen, mit denen die Nutzung von Datenverarbeitungssystemen durch Unbefugte verhindert wird:

- Zugangsschutz (Authentisierung)
- Authentisierung der Mitarbeiter (per Benutzername/Passwort) bei hohem Schutzniveau
- Personen mit Zugangsberechtigungen werden explizit bestimmt und auf ein Minimum beschränkt
- Personengebundene Authentisierungsmedien werden dokumentiert und verwaltet
- Protokollierung der erfolgreichen und abgewiesenen Zugangsversuche
- Festlegung befugter Personen
- Automatische und manuelle Zugangssperre bei Verlassen des Arbeitsplatzes

c) Zugriffskontrolle (Vertraulichkeit – Art. 32 Abs. 1 lit. b DSGVO)

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugangsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Berechtigungskonzept
- Umsetzen von Zugriffsbeschränkungen
- Vergabe minimaler Berechtigungen
- Personengebundene Zugriffsberechtigungen werden verwaltet und dokumentiert
- Protokollierung des Datenzugriffs

d) Weitergabekontrolle (Integrität – Art. 32 Abs. 1 lit. b DSGVO)

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- Protokollierungen jeder Übermittlung oder einer repräsentativen Auswahl
- Sichere Datenübertragung zwischen Server und Client
- Sicherheitsgateways an den Netzübergabepunkten
- Die Datenspeicherung erfolgt ausschließlich auf der Plattform und dem Backup-System

- Die vollständige, datenschutzgerechte und dauerhafte Löschung von Daten bzw. Datenträgern mit Kundendaten des Auftraggebers wird protokolliert.

e) Eingabekontrolle (Integrität – Art. 32 Abs. 1 lit. b DSGVO)

Maßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind:

- Die Dateneingabe erfolgt ausschließlich durch den Kunden

f) Auftragskontrolle (Art. 32 Abs. 1 lit. d DSGVO)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Kunden verarbeitet werden können:

- Die Daten werden nur entsprechend der „Lizenz- und Nutzungsbedingungen für die Software CompuDMS Cloud“ und auf Weisung des Kunden verarbeitet.

g) Verfügbarkeitskontrolle (Verfügbarkeit u. Belastbarkeit – Art. 32 Abs. 1 lit. b DSGVO)

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- CompuKöln betreibt ein automatisiertes 24 h / 365 Tage IT-Überwachungssystem
- CompuKöln führt in der Regel tägliche Backups der relevanten Informationen durch. Darüber hinaus ist der Kunde verpflichtet, Sicherungskopien seiner Daten vorzuhalten. Diese können mit den entsprechenden Funktionen von CompuDMS Cloud erstellt werden.

h) Trennungskontrolle (Vertraulichkeit – Art. 32 Abs. 1 lit. b DSGVO)

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Die Daten der Kunden werden voneinander getrennt abgelegt und verarbeitet.

i) Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

Maßnahmen, die gewährleisten, dass eingesetzte Systeme im Störfall wiederhergestellt werden können.

- Es existieren Pläne und Dokumentation um – unter Berücksichtigung des Stands der Technik, der Implementierungskosten und des vom Kunden entrichteten Entgeltes – einen raschen Wiederanlauf zu ermöglichen.

k) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

- Die in dieser Anlage genannten Maßnahmen werden durch den Datenschutzbeauftragten der CompuKöln, den Sicherheitsbeauftragten der CompuKöln, die Geschäftsführung der CompuKöln sowie jeden mit der Betreuung des Systems beauftragten Mitarbeiter der CompuKöln kontinuierlich überwacht und geprüft.